Information Privacy in the Evolving Healthcare Environment

Edited by
Linda Koontz, CIPP/US, CIPP/G

HIMSS®

Information Privacy in the Evolving Healthcare Environment

Edited by
Linda Koontz, CIPP/US, CIPP/G

HIMSS Mission
To lead healthcare transformation through effective use of health information technology.

Printed in the U.S.A. 5 4 3 2 1

Requests for permission to make copies of any part of this work should be sent to:
Permissions Editor
HIMSS
33 West Monroe Street, Suite 1700
Chicago, IL 60603-5616
mschlossberg@himss.org

ISBN: 978-1-938904-36-3

For more information about HIMSS, please visit www.himss.org.

About the Editor

Linda Koontz, CIPP/US, CIPP/G

Ms. Koontz is a Senior Principal for Privacy and Strategy at MITRE, a not-for-profit corporation chartered to work solely in the public interest, where she advises senior-level staff at federal agencies on strategic approaches to building privacy into their organizations, processes, and systems. Drawing from her more than 30 years' experience in information systems and technology, she currently advises the Chief Privacy Officer of the Office of the National Coordinator on privacy issues associated with nationwide implementation of health information exchange and manages the activities of the Health Information Technology Policy Committee's Privacy and Security TIGER Team. She has also provided privacy advice and support to the Department of Homeland Security and was recently appointed by the Secretary to the Department's Data Protection and Integrity Advisory Committee (DPIAC).

Before joining MITRE, Ms. Koontz served as the Director, Information Management, for the U.S. Government Accountability Office (GAO). In that role, she directed a broad portfolio of congressionally-requested studies, producing numerous reports on privacy, information access and dissemination, information collection, and records management. Ms. Koontz also testified numerous times before congressional committees as an expert witness on these issues.

She holds a BA in Accounting from Michigan State University and is a Certified Information Privacy Professional. She also is an Executive Coach and a graduate of Georgetown University's Leadership Coaching Program.

About the Contributors

Robert Belfort, JD, is Partner at the law firm Manatt, Phelps & Phillips, LLP. He advises hospitals, community health centers, medical groups, managed care plans, and other healthcare stakeholders on regulatory and transactional matters. He assists clients with managing health information in compliance with HIPAA and state confidentiality laws and advises on Stark law, anti-kickback and other fraud and abuse matters.

Linda Dimitropoulos, PhD, is Director of the Center for the Advancement of Health IT at RTI International. Dr. Dimitropoulos is a social psychologist with expertise in attitude change and persuasive communications applied to consumer behavior and decision making. She has led the privacy and security solutions for Interoperable Health Information Exchange project, and the Health Information Security and Privacy Collaboration (HISPC), and serves as a Senior Advisor on the State Health Policy Consortium project. She has served on many technical expert panels, including health IT and mental health: the Path Forward, sponsored by the Agency for Healthcare Research and Quality (AHRQ), and the National Institute of Mental Health (NIMH).

Leslie Francis, PhD, JD, is Associate Dean for Faculty Research & Development, Alfred C. Emery Distinguished Professor of Law, and Distinguished Professor of Philosophy at the University of Utah. She also holds adjunct appointments in the departments of Internal Medicine (Medical Ethics), Political Science, and Family and Preventive Medicine (Public Health). Dr. Francis co-chairs the subcommittee on Privacy, Confidentiality, and Security, U.S. National Committee on Vital and Health Statistics (NCVHS advises HHS and CDC on issues of health data and population statistics) and is an elected Vice-President of the International Society for the Philosophy of Law and Social Philosophy (IVR).

Lisa A. Gallagher, BSEE, CISM, CPHIMS, serves as HIMSS' Senior Director of Privacy and Security. In this role, she is responsible for all of the privacy and security programs and provides privacy and security content support for HIMSS' federal and state government relations/advocacy work. Ms. Gallagher currently serves on the ONC Standards Committee's Privacy and Security Work Group and the Patient Matching Power Team. Ms. Gallagher has a Bachelor of Science degree in Electrical Engineering, was a certified trust technology evaluator (NSA), and is a Certified Information Security Manager (CISM) (ISACA). She is also a Certified Professional in Healthcare Information and Management Systems (CPHIMS).

Kimberly S. Gray, Esq., CIPP/US, is the global chief privacy officer of IMS Health, the world's leading provider of market intelligence to the pharmaceutical and healthcare industries. She is responsible for the development, oversight, and promotion of IMS Health's comprehensive privacy, data protection, and data management program, which includes policy development, communications and strategic direction for the company. Ms. Gray serves on the Ponemon Institute's RIM Council, the Centre for Information Policy Leadership (CIPL), the Ethics Committee of the European Pharmaceutical Market Research Association (EphMRA), the Confidentiality Coalition of the Healthcare Leadership Council, and the Executive Council of HITRUST. She has served on the Board of Directors of the International Association of Privacy Professionals (IAPP) and continues to be actively involved with IAPP. She is also an active member of the American Health Lawyers Association and the American Bar Association's Health Law Section. Ms. Gray holds a Juris Doctor from The Dickinson School of Law of Pennsylvania State University. She lectures frequently on privacy and information security issues.

Susan Ingargiola, MA, is Director at Manatt Health Solutions. She provides strategic business, regulatory, and reimbursement advice to healthcare providers, nonprofit organizations, and pharmaceutical/biotechnology companies. She specializes in health information privacy and confidentiality laws and health information technology.

John Mattison, MD, is privileged to have played a small part in implementing the pioneering vision of Dr. Sidney Garfield, founder of the revolution led by Kaiser Permanente for the past 60 years, blessed to have learned from and shared that opportunity with Ken Murtishaw and Diana Villania and many other world class managers, and grateful to be living in the most creative and disruptive era in the history of the caring professions.

Julie S. McEwen, CIPP/G/IT/US, CISSP, PMP, is a Principal Privacy and Cybersecurity Engineer and leads the privacy capability at the Cybersecurity and Privacy Technical Center at MITRE. She is currently working on privacy research in the healthcare area, and has also supported the U.S. Department of Health & Human Services. Prior to joining MITRE, she managed privacy and cybersecurity programs and advised organizations on policy and technology issues while at the U.S. Department of Defense, Deloitte, IIT Research Institute, the Logistics Management Institute, and T. Rowe Price. She is editor of *U.S. Government Privacy: Essential Policies and Practices for Privacy Professionals*.

Kris Miller, JD, MPA, CIPP/G, is a Lead Privacy Strategist at MITRE, a not-for-profit technology consultancy that services the U.S. government. In this role, Mr. Miller has been a trusted advisor to government leaders regarding privacy compliance, policy development, and strategic planning. He has supported the Office of the Secretary of Defense, the Centers for Medicare & Medicaid Services, the Veterans Benefits Administration, and the Department of Homeland Security. Prior to joining MITRE, Mr. Miller represented public and private companies as a corporate attorney in the New York City area. Before practicing law, Mr. Miller served as a Captain in the U.S. Army. Mr. Miller earned his Bachelors degree from Boston University, his Master's degree in public administration from the Maxwell School of Citizenship and Public Affairs, and his law degree from the Syracuse University College of Law. He is a Certified Information Privacy Professional with a specialty in government privacy (CIPP/G) and a licensed member of the bar in both Connecticut and New York.

Larry Ozeran, MD, is a surgeon and software developer. He was a UC Davis associate faculty in informatics for three years and an editor of *H.I.T. or Miss* (AHIMA, 2010). He has recorded popular HIMSS podcasts on health IT failure and ARRA and serves on the HIMSS Public Policy Committee. Dr. Ozeran is an AMIA Working Group chair and served on the AMIA Public Policy Committee. He received an award from the State of California for assisting in its response to ARRA, later advising Cal eConnect and CalHIPSO. President of Clinical Informatics, he advises clients on public policy, strategic planning, provider engagement, and clinician training.

Deborah C. Peel, MD, is a leading U.S. advocate for patients' rights to control access to sensitive personal health information in electronic systems. In the United States, the lack of health information privacy causes millions of Americans every year to avoid early diagnosis and treatment for cancer, depression, and STDs. She is also a practicing physician and has been a Freudian psychoanalyst for more than 30 years. She founded Patient Privacy Rights (PPR), the nation's leading consumer health privacy advocacy organization, which defends Americans' rights to health privacy. PPR has 12,000 members in all 50 states. She also leads the bipartisan Coalition for Patient Privacy, representing 10.3 million people. Dr. Peel created and hosts the International Summits on the Future of Health Privacy. The summits bring together national and international experts from advocacy, academia, government, and industry to debate urgent problems and compare solutions. Academic partners have included the University of Texas LBJ School of Public Affairs, the O'Neill Institute at Georgetown Law Center, the University of Cambridge Computer Lab, the Harvard Data Privacy Lab, and the University of Texas School of Information. Dr. Peel was named one of the "100 Most Influential in Healthcare" in the United States by *Modern Healthcare* in 2007, 2008, 2009, and 2011—the first and only privacy expert and advocate on the list.

Contents

Acknowledgments

I would like to thank the chapter authors for generously sharing their expertise and engaging in a virtual, months-long discussion on this book. I enjoyed the journey with you all. I would also like to thank the staff of HIMSS, especially Lisa Gallagher, and our HIMSS editor, Matt Schlossberg, who provided expert advice and guidance at every step throughout this process.

I would also like to thank my employer, MITRE, for agreeing that a book on health information privacy was part of its mission to work in the public interest and for supporting my work as an editor and author. In particular, I would like to thank Joy Keeler Tobin as the champion for this project and my colleagues Marie Muscella and Lisa Tutterow. Kimberly Nesbitt also provided invaluable help to the editing process for this book—thank you sincerely for your insightful advice and assistance.

Finally, I would like to thank my husband Dan, and my sons Nick and Ryan for their patience and their willingness to just listen.

—Linda Koontz, CIPP/US, CIPP/G

Introduction

By Linda Koontz, CIPP/US, CIPP/G

As someone who has studied information privacy for many years, privacy in the healthcare domain has always held significant interest for me. First of all, it is *tremendously important* because of what is at stake. According to Centers for Medicare & Medicaid Services (CMS) actuaries, healthcare costs are expected to grow an average of 5.7 percent per year between 2011 and 2021.[1] Further, studies have shown that while the United States spends more on healthcare than other industrialized nations, it lags behind in performance and outcomes.[2,3] These developments make it clear that we must continue to look for ways to improve patient care and the healthcare system itself using a variety of means, including through the adoption of health information technology. However, the ability to successfully leverage the potential of health IT depends to a large degree on the public trusting that their information will be kept private and secure. Secondly, *health information privacy is incredibly complex* and challenging. Electronic health records and the exchange of health information are still in their nascent stages and significant work and original thinking still remain to be done in the coming years to integrate and balance technology, privacy, security, and the delivery of healthcare. The scope of this issue is also enormous, potentially affecting the way that not only every healthcare provider, hospital, and insurer collect, use, and share personal health information, but also how patients will access their own information and ultimately, how they will interact with their healthcare providers.

What I have found over time in studying privacy and advising the federal government on privacy issues is that while individuals clearly value privacy, there is at the same time a great deal of confusion over the subject. We are all familiar with anecdotes of privacy "rules" being used to unnecessarily withhold information from the people who need it. In addition, many mistake keeping information secure—that is, confidential and safe from unauthorized disclosure—as being the same as preserving individuals' right to privacy. Thus, this book is intended to educate a broad audience on the meaning of privacy and the challenges facing our nation as we move to improve our healthcare system. My goal is simply to describe privacy and its associated challenges in the healthcare domain, not only to other privacy professionals who are passionate about privacy, but primarily to physicians and other healthcare providers, people in the business end of healthcare, information technology professionals, policymakers, and patients.

This book is divided into three parts. The first four chapters lay the foundation by exploring the meaning of privacy, the relationship between privacy and medical ethics, the synergy that exists between information privacy and security, and the complex legal

landscape governing health information privacy. The middle of the book, Chapters 5 through 10, explore some of the most significant privacy challenges faced by the healthcare community as it seeks to transform itself. The topics span the gamut from health information exchange to consent to secondary use to transparency. The final chapter looks to the future, identifying current trends and providing a view of the changes we might expect to see as a consequence of these trends.

The expert authors of the various chapters in this book represent a diversity of disciplines as well as thought. Among them are physicians, researchers, policy analysts, lawyers, privacy practitioners, and privacy advocates. Given this diversity, however, the reader may note that there are differences in how the various authors describe privacy and in the solutions they are proposing to the challenges that face us. These are not contradictions as much as a reflection of the reality of the multiple meanings of privacy, and that in many ways, we are still at the beginning of a very long discussion on this subject. My hope is that the reader will walk away with a greater understanding of privacy, the issues in healthcare, and an appreciation of the range of viewpoints and options that exist.

References

1. Office of the Chief Actuary, Centers for Medicare & Medicaid Services (CMS). National Health Expenditure Projections 2011-2021; 2012. Available at: www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf. Accessed on September 30, 2012.
2. Davis K, Schoen C, Stremikis K. Mirror, Mirror on the Wall: How the Performance of the U.S. Health Care System Compares Internationally, 2010 Update, The Commonwealth Fund; June 2010. Available at www.commonwealthfund.org/~/media/Files/Publications/Fund%20Report/2010/Jun/1400_Davis_Mirror_Mirror_on_the_wall_2010.pdf. Accessed on September 30, 2012.
3. Kaiser Family Foundation. Health Care Spending in the United States and Selected OECD Countries; April 2011. Available at www.kff.org/insurance/snapshot/oecd042111.cfm. Accessed on September 30, 2012.

Chapter 6

An Implementation Path to Meet Patients' Expectations and Rights to Privacy and Consent

By Deborah C. Peel, MD

The United States has a long history of medical ethics and strong laws that ensure patients' control of their medical records. However, gaps in current U.S. law and flaws in health IT give data holders disproportionate control over the use, disclosure, and sale[1] of sensitive health information.[2-5] Further, there is no map of health data flows which could provide the public with greater transparency on how their sensitive health information is used and shared.[6] As a result, many uses of patients' sensitive health information are hidden from their view.

The standard of practice for physicians has been to obtain consent before using or disclosing health information, but effective, meaningful consent is not embedded in current health technology systems.[7] This is particularly problematic because the right of consent is the foundation for patient trust in physicians and healthcare systems.[8] Without trust, people avoid treatment[9] and hide sensitive information[10] about their minds and bodies.

Innovative privacy-enhancing technologies and robust trust frameworks[11] could enable exquisitely granular electronic consent,[12] even down to the data field level, and put patients back in control of personal health information. Then patients could move the right information to the right person at the right time, and prevent health data from being sold or used for purposes with which they do not agree.

Technology can unquestionably provide enormous benefits to the nation's health, but only if we strengthen requirements governing consent, restore patients' control over their information, and build meaningful consent and trust frameworks[13] into electronic systems and data exchanges.

This chapter will cover patients' right to privacy and consent. Specifically, it will include discussions of the origin of consent; legal and ethical rights to consent; the need for greater patient control over PHI;[14] current best practices for electronic consent; new initiatives that could lead to greater patient control over PHI; and a five-year implementation plan for health IT systems and data exchanges based on consent and trustworthy privacy frameworks.

ORIGINS OF CONSENT AND THE RIGHT TO THE PRIVACY OF HEALTH INFORMATION

The National Committee on Vital and Health Statistics (NCVHS) defines health information privacy as "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."[15] Though Congress and HHS have yet to adopt a definition of privacy, the concept of privacy as control over personal information is embedded in American law.[16-19] Equally important, patients believe that each individual should be able to make his or her own decisions regarding who can see and use personal health data.[20] Controlling PHI by giving or withholding permission to collect, use, disclose, delete, or sell it is known as the "right of consent."

Hippocrates understood the conditions needed to trust another person and share sensitive information. Key among the ethical principles in the Hippocratic Oath is the requirement that physicians keep sensitive information private. The oath to honor and respect patients' privacy and autonomy by protecting information about them has been the basis for trust in physicians for more than 2,400 years, and is the basis for Americans' legal rights to health privacy.

The legal framework for consent and health privacy rights in the United States was developed over the course of 200 years in every state and the District of Columbia. It consists of federal and state law, common law, tort law, and Constitutional decisions and rights. There is a strong national consensus that individuals should have a right to health information privacy and a right of consent.

Summary of Americans' Privacy and Health Privacy Rights

The strongest privacy protections are in state laws, which contain protections for sensitive health information (cancer registries, sexually transmitted diseases, genetic and mental health data, etc.), federal court decisions, and Supreme Court decisions. Although a few states have eliminated longstanding, stronger health privacy protections by passing legislation to harmonize state requirements with HIPAA's, most have not.

States also recognize in tort and common law a right to privacy for personal health information.[21] Ten states have a right to privacy expressly recognized in their constitutions; other states' Supreme Court decisions recognize that residents have a right to privacy. A physician-patient privilege is recognized in 43 states and the District of Columbia.[22] The "reasonable expectation" of privacy for health information has been recognized repeatedly by courts at every level. Further, the ethical codes of all health professions require informed consent before use or disclosure of personal health information.[23] American Medical Association (AMA) policy states that where possible, "informed consent should be obtained before personally identifiable health information

is used for any purpose."[24] Consequently, many states require adherence to the Code of Medical Ethics as a licensure requirement for physicians. Finally, a psychotherapist-patient privilege is recognized in all 50 states and the District of Columbia.[25]

Several federal laws also set strong health privacy precedents:

- **42 CFR Part 2,** the Public Health Regulations on the Confidentiality of Alcohol and Drug Abuse Patient Records,[26] requires informed consent for the disclosure of alcohol and substance abuse treatment records.
- **Title 38 Part V, Chapter 73, Subchapter III, Protection of Patient Rights, 7332,** requires consent before records of drug abuse, alcoholism or alcohol abuse, HIV, or sickle cell anemia are disclosed outside of the military health system.
- **HIPAA** allows providers to offer a consent process before disclosing PHI and requires consent before the disclosure of "psychotherapy notes."
- **HITECH** requires that patients who pay privately for treatment must be able to prevent PHI from being disclosed to health plans.

Americans also have strong Constitutional rights to privacy and health information privacy. The Constitutional right to privacy grew from Justice Brandeis' 1928 dissent in *Olmsted*.[27] He famously wrote, "The right to be let alone is the most comprehensive of rights and the right most valued by civilized men." The right to privacy of highly personal information is protected under the right to be free of unreasonable searches and seizures under the Fourth Amendment, and the right to liberty under the Fifth and Fourteenth Amendments to the U.S. Constitution.[28] The right to privacy of personal information also has been recognized by Congress and by HHS as a fundamental constitutional right.[29] The right to "informational privacy," i.e., the right of an individual to have his personal information kept private,[30] grew from *Whalen v Roe* in 1977.[31] Finally, the U.S. Supreme Court established a psychotherapist-patient privilege in 1996.[32] "The mere possibility of disclosure may impede the confidential relationship necessary for successful treatment."[33] Failure to protect the right to health information privacy leads to less health information because communications between practitioners and patients "would surely be chilled."[34]

Why Consent Is Important

For patients, privacy is a simple question: do I care if a certain person sees or uses my health information or not? Privacy comes down to the expectation that each person should have the power to make his/her own decisions about who sees and uses personal health information, rather than be subject to one-size-fits-all rules.[35]

In 2011, Professor Alan F. Westin reviewed 95 surveys published over 20 years about public attitudes toward privacy and technology.[36] According to Westin's research, 25 percent of the public is "Privacy Intense," but 35 percent to 40 percent is "*Health* Privacy Intense" and have strong concerns about:

- Secondary uses of health data, by insurers, employers, and government programs.
- Research access to personal health data without notice and direct consent.
- Discrimination against persons with potentially stigmatizing conditions.

Further, they are "not impressed by voluntary practices" and "want legal controls and strong regulatory enforcement." These individuals, as well as others who do not trust or use online platforms because of the lack of privacy,[37] will only trust health IT if they control routine uses of health data for healthcare operations TPO.

The Evolution of Consent and the Privacy Rule

In 2001, HHS issued the HIPAA Privacy Rule to implement the privacy provisions of HIPAA. Patient consent was required before any information could be shared:

> ….a covered health care provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.[38]

In 2002, HHS amended the HIPAA Privacy Rule, eliminating the right of consent for treatment, payment, and healthcare operations:

> The **consent provisions…are replaced** with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations.[39]

This massive change turned HIPAA from a "Privacy Rule" to a "Disclosure Rule." More than 4 million covered entities (CEs)—providers, health plans, and clearinghouses—were granted broad rights to control the nation's protected health information; neither consent nor advance notice were required.

HHS argued that patients expect CEs to use PHI for treatment and claims payment. This position does not reflect patients' decisions to selectively share information with health professionals or to pay privately to prevent insurers' access to PHI. Patients do not tell allergists about sexual problems and typically do not share mental health information because physicians often react negatively.[40] Further, few people know that PHI is used for "healthcare operations" or what that means. This broad data-use category is subject to abuse. These changes in HIPAA were not widely reported and, to this day, most people are unaware that the right of consent was eliminated, and CEs and other institutions now control the use of health data.

As HHS explained when issuing the Amended HIPAA Privacy Rule in 2002:

> The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force. In order to not interfere with such laws [affording a right of consent] and ethical standards, this Rule permits covered entities to obtain consent. Nor is the Privacy Rule intended to serve as a 'best practices' standard. Thus, professional standards that are more protective of privacy retain their vitality.[41]

The HIPAA Privacy Rule also permits disclosures of PHI without consent for many categories of use.[42] "A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations:

- To the individual (unless required for access or accounting of disclosures).

- Treatment, payment and healthcare operations.
- Opportunity to agree or object.
- Incident to an otherwise permitted use and disclosure.
- Public interest and benefit activities.
- Limited data set for the purposes of research, public health or healthcare operations.

Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make."

"Public Interest and Benefit Uses"[43] include 12 broad categories of use permitted without authorization required by law:

- Public health activities
- Victims of abuse
- Neglect or domestic violence
- Health oversight activities
- Judicial and administrative proceedings
- Law enforcement purposes
- Decedents
- Cadaveric organ, eye, or tissue donation
- Research (quite broad)
- Serious threat to health or safety
- Essential government functions (e.g, military and veterans' activities, national security and intelligence, protective services for the President and others, medical suitability determinations for government jobs, correctional institutions and other law enforcement custodial situations, covered entities that are government programs providing public benefits).
- Workers' compensation

All other uses and disclosures require patients' written authorization.

NEED FOR GREATER PATIENT CONTROL OVER HEALTH INFORMATION AND ELECTRONIC CONSENT

The lack of adequate consent in health IT systems causes harms. Patients put their health and lives at risk by hiding information or avoiding treatment to prevent sensitive health information from being disclosed.

Millions of Patients Hide Information Every Year

The California Healthcare Foundation found that 13 percent to 17 percent of consumers engage in information-hiding.[44] One in eight Americans puts their health at risk because of privacy concerns. These individuals take the following actions:

- Avoid seeing their regular doctor.

- Ask their doctor to alter a diagnosis.
- Pay for a test out-of-pocket.
- Avoid tests.

Millions of Americans Avoid Treatment Every Year

Many patients' health records have been disclosed to employers and others. Surveys, like one in 2012 by the California Healthcare Foundation, found that 68 percent of Americans are concerned about the privacy of medical records.[45] Because privacy concerns are not addressed in today's electronic health systems, real harm occurs now. Patients avoid care, suffer, and even risk death.

- HHS estimated that 586,000 Americans did not seek early cancer treatment due to privacy concerns.[46]
- HHS estimated that 2 million Americans did not seek treatment for mental illness due to privacy concerns.[47]
- Millions of young Americans suffering from sexually transmitted diseases do not seek treatment due to privacy concerns.[48]
- The Rand Corporation found that 150,000 soldiers suffering from post traumatic stress disorder (PTSD) do not seek treatment because of privacy concerns.[49]

The lack of privacy contributes to the highest rate of suicide among active duty soldiers in 30 years.[50] In 2011, for the first time, deaths by suicide exceeded deaths on the battlefield.[51,52]

As the public learns how little control they have over health information in electronic systems and data exchanges, millions more may avoid treatment for serious diseases and hide information. Bad health outcomes unintentionally created by current technology systems can only be addressed by implementing privacy frameworks and restoring the patient's control over use and disclosure of PHI.

TECHNOLOGY-ENABLED DISCRIMINATION BASED ON HEALTH AND GENETIC INFORMATION

"As growing technological prowess enables sophisticated discrimination capabilities, our reach for health and economic benefit [by allowing broad access to PHI without consent] stands to collide with the ethical core of medicine."[53]

Most patients expect their doctors will do the right thing and keep their records private. Few patients are aware that as soon as health information is entered into health IT systems, the disclosure, misuse, and sale of this personal information by users can begin. For example, many EHR vendors and hospitals sell or use patient data[54] in ways patients do not expect. Surveys show that individuals have a "common belief" and "strong expectation" that their personal health information will not be disclosed without their consent.[55] A map of health data flows is essential to understanding how health information-based discrimination happens.[56]

Thirty-Five Percent of Fortune 500 Companies Use Medical Records for Hiring and Promotions[57]

Concerns about the use of health information to discriminate against people in jobs, credit, and employment are documented in many polls.[58-60] Physicians, such as psychiatrists and oncologists, who treat patients with stigmatizing or expensive diseases commonly see discrimination. According to William Pewen, PhD, former health policy advisor to Sen. Olympia Snowe (R-ME), "Advancing technology was opening a virtual Pandora's Box of new civil-rights challenges. At the crux of these was the fact that scientific progress has been enabling increasingly sophisticated discrimination."

Further, he wrote, "Our experience with the Genetic Information Nondiscrimination Act (GINA) helped to reveal the tip of an emerging threat—the use of modern data systems to create new forms of discrimination—and our concern focused on the use of personal medical data. While genetic data expresses probabilities, other parts of one's medical record reflect established fact—an individual's diagnoses, the medications one has used, and much more."[61]

Pewen also described how technology-based discrimination works and made the case that selling health information profiles is the business model for many technology corporations. In his words, "Millions [of people] are beginning to recognize that they are not the customers, but the product."[62]

LACK OF CONSENT ADVERSELY AFFECTS RESEARCH

The Institute of Medicine's (IOM) 2007 Project Survey Findings on Health Research and Privacy[63] reported**:**

- 1 percent of the public would allow unfettered research access to PHI without consent.
- 8 percent would be willing to provide general consent for use of their health information in advance for future research project.
- 19 percent of the public would allow researcher access to their information without consent as long as the study never revealed their personal identity and the research was supervised by an institutional review board (IRB).
- 38 percent wanted researchers to obtain their consent for each individual research project.
- 13 percent did not want to be contacted or have their information used in any case.
- 20 percent indicated that they were "not sure" of which of the above statements they agreed with most.

Although the HIPAA Privacy Rule[64] requires authorization (consent) for research use of PHI, it also allows use without consent with a waiver from an IRB or privacy board. However, as the IOM study shows, many members of the public are not comfortable with research use of EHRs without consent.

'Data Hiding' Affects the Quality and Reliability of Research

Millions of patients every year omit data or lie to protect the privacy of sensitive information,[65] causing gaps and errors in EHRs. Errors and omissions limit the usefulness of data for research and may also cause treatment errors. When data used for research are unreliable, research conclusions may be unreliable.

Unreliable data interferes with developing accurate "outcomes" measures, quality measures, accurate information about population health, and learning which treatments are "comparatively" most effective, etc. Today millions of patients get treatment off-the-grid by paying out-of-pocket for care or avoid treatment altogether, so critical data cannot be collected. Millions of people pay out-of-pocket for psychotherapy or psychoanalysis, or join Alcoholics Anonymous. But there are no electronic records of these effective treatments.

Unless informed consent is required for research and public health uses of PHI, as it is in many contexts by stronger federal and state laws, the Common Rule, ethical codes for research,[66] and international treaty,[67] patients may avoid treatment fearing their data will be used for research they do not support.

HIPAA's provisions allowing the use of PHI for public health also exceed the public's expectations. HHS greatly expanded public health access to PHI in the HIPAA Privacy Rule by granting public health entities access to *all* patient data. Before HIPAA, public health authorities could track personal information only on people with certain infectious diseases like tuberculosis (TB) and HIV/AIDS, as mandated by state or federal law. Yet "the Privacy Rule continues to allow for the existing practice of sharing PHI with public health authorities who are authorized by law to collect or receive such information to aid them in their mission of protecting the health of the public."[68]

Research ethics require that "the well-being of the human subject should take precedence over the needs and interests of society."[69] Researchers and public health authorities can earn trust and goodwill, and get more accurate and complete data by seeking consent for research use or public health use of PHI. Technology can dramatically improve the ease and quality of consent so that the public will trust and be willing to participate in clinical and public health research. People actually disclose more accurate and complete information when they know they control the use of their information.

WHY ELECTRONIC CONSENT TOOLS ARE NECESSARY

Patients Will Be Able to Trust Health IT

When electronic consent enables patients to control the use and disclosures of PHI, they will not need to hide sensitive information or delay critical treatment to keep health data private. They will be able to protect themselves from discrimination by preventing hidden use of health and genetic data. Finally, consent tools will allow patients to donate data for research they support and know that PHI cannot be used for research without their permission.

Benefits of Consent

Innovative electronic consent systems can educate and test consumers' understanding of informed consent; the risks and benefits of participating in treatment, surgery, or clinical trials;[70] or donating data for research.[71] It makes sense to use technology to improve consent and patients' understanding of how PHI will be used and shared.[72]

- **Convenience**: Patients can review consent online anytime.
- **Less pressure and anxiety**: Can review the consent form and consult with family members without feeling pressure to sign right away.
- **More informed**: Participants can review the consent form at their leisure, allowing them to make a more informed decision and better understand the research, treatment, uses, or disclosures.
- **More engaged**: Electronic consent technologies can be more engaging than paper consent documents.
- **Improve comprehension:** By incorporating non-linear text and non-text mediums:
    - **Non-linear text** allows a self-directed, associative learning experience. For example, hypertext allows readers to easily click on a term in an informed consent document, which could present a definition or more information about a term.
    - **Non-text communication mediums** such as video or interactive graphics could lead to more informed participants.

Burdens Created by Paper Consent Forms Will Be Eliminated for Patients and Data Holders

Problems created by paper consent forms include[73]

- Patients cannot specify their privacy directives in one place.
- Paper forms are legalistic, not user-friendly, and not interactive or educational.
- Future referrals or secondary uses of data, such as for research and public health, cannot be addressed.
- Granular restrictions are absent or limited; patient choices are limited to what providers find convenient.[74]
- Patients cannot easily identify and revoke multiple paper consents.
- Maintaining stacks of paper consents is costly and inefficient for record holders.
- Record holders must seek consent and negotiate with multiple record holders for access to PHI.
- Paper forms are not current; record holders must locate the most current form or wait and obtain a new consent.
- Record holders must attach conditions to data they export and interpret conditions attached to data they receive.

Best Practices in Meaningful Consent

The most critical factor for patient trust in electronic health systems and data exchanges is the ability to decide who can see and use personal health data. Consent models should be meaningful and patient-centered, which can only be accomplished with consent management technology. Electronic consent systems enable patients to set customized broad and narrow personal directives for data use and disclosure; are convenient; are easy to use, change, and understand; are located in one place so all data holders can instantly learn each patient's latest rules; and comply with patients' expectations and legal and ethical rights.

To be "meaningful," consent[75] must:

- Allow time for informed decisions.
- Not be required for treatment or data exchange, or allow data use for discrimination.
- Be transparent, comprehensible, and clearly explain all choices and consequences.
- Fully inform patients when sensitive information or data are used in ways that do not comply with patients' expectations or rights.
- Be consistent with patients' expectations and rights for privacy, health, and safety.
- Be easily revocable.

BEST PRACTICES: CURRENT EXAMPLES OF MEANINGFUL INFORMED CONSENT

The following models of consent at the Harvard Personal Genome Project, MD Anderson Cancer Center, and at public mental and substance abuse treatment centers show that electronic and multimedia consent can educate patients, offer more complete information about risks and benefits of data disclosure than traditional paper consent, enable patients to customize disclosures, and reduce the burden of collecting and managing paper consents.

The Multimedia Consent Process for the Harvard Personal Genome Project (PGP)

PGP[76] requires about 90 minutes, watching a video, and scoring 100 on a test of comprehension of the risks and benefits of putting your genome and PHI online to allow downloads for research or other purposes. The PGP takes great pains to ensure data donors understand the "known and unknown" risks that could result: "The risks of public disclosure of your genetic and trait information could affect your employment, insurance and financial well-being and social interactions for you and your immediate family." A "non-comprehensive" list of hypothetical scenarios that could pose risks to participants and families is included.

> The PGP's informed consent process accurately and comprehensively explains current data privacy and security risks and potential harms. The PGP lists key risks for health data in all electronic systems:

- **Risk of "significant loss of privacy** and personal time."
- "Whether or not it is lawful to do so, you could be **subject to actual or attempted employment, insurance, financial or other forms of discrimination or negative treatment** on the basis of the public disclosure of your genetic and trait information by the PGP or by a third party."
- "**Any data or other information you may have shared pursuant to a promise of confidentiality or privacy may become public** despite your intent that it be kept private and confidential…this could result in certain adverse effects for you, including ones not contemplated by this consent form."
- "**The complete set and magnitude of the risks that the public availability of this information poses to you and your relatives is not known at this time**. You are strongly encouraged to discuss this study and its potential risks with your immediate family members."

MD Anderson Cancer Center

MD Anderson Cancer Center[77] has offered targeted therapies, surgery, chemotherapy, radiation and proton therapy, immunotherapy, or combinations of treatments to over 900,000 patients since 1941. In 2011, more than 108,000 people sought care at MD Anderson. MD Anderson was an early adopter of EHRs[78] and "Blue Button," a function that allows patients to view and download their health information. MD Anderson uses many best practices for consent and EHRs including:

- Separate opt-in informed consents for research and treatment are embedded in the EHR system.
- Patients can always access and review their signed consent forms online. The MD Anderson staff is careful to obtain consent in person, rather than obtaining rushed "front door" consents during admission.
- Separating the consent process for research and treatment: as a matter of ethics and respect for patient autonomy, the Center takes the position that vulnerable patients should not feel coerced to participate in research.
- Since 2009 MD Anderson Cancer Center has been providing patients with online access to EHRs, and to their families and referring physicians with consent. This is one of the first instances of enabling "Blue Button" downloads of PHI by patients and those they trust.
- Patients can request a complete list of those who received copies of their medical records. Plans are underway to make the list available immediately or whenever patients want it, and list the specific data released.

The National Data Information Infrastructure Consortium Model

The National Data Information Infrastructure Consortium (NDIIC) is a "virtual non-profit organization primarily supporting the field of behavioral health services by offering a range of services to assist states, sub-state entities, and community-

based organizations in software acquisition, consultation, development, and training. The primary goals of NDIIC include ongoing collaboration and open sharing of information on behalf of its members."[79] State NDIIC members pooled their resources to build open source EHRs and robust consent technologies that comply with 42 CFR Part 2. The resulting modular electronic consent technology developed by the NDIIC is one of the best *existing* models for consent in widespread use. It includes robust, granular choices for selective disclosures of mental health and substance abuse data,[80] and more than 50 consumer choices for data segmentation, time limits, and selection of recipients.[81] (See Appendix III for these consent components.) The model has been used for over 13 years in at least nine state mental health systems and 22 state and regional jurisdictions.[82] In 2010, one version was demonstrated at the National HIT Policy Committee's Consumer Choices Technology Hearing.[83]

To date, over four million records have been exchanged by large and small provider organizations and across large and small states and counties generating and exchanging data point-to-point, using meaningful, informed consent. Patients' consent choices are electronically filled out by providers who consult with each patient about which portions of their records to disclose to others. The next step the government should make is to create patient and physician portals and electronic consent tools so patients can enter their own consent directives and exercise their rights to control PHI.

PROMISING CURRENT INITIATIVES FOR PATIENT ACCESS TO AND CONTROL OVER PHI

By permitting patients' greater control over PHI and data exchange, the following projects will inevitably usher in the future, when patient-controlled healthcare systems replace current industry and institutionally-controlled healthcare systems.

The Direct Project[84]

Today, the only method of data exchange that could potentially *quickly* enable patients to control routine uses and disclosures of PHI is the Direct Project. "The Direct Project specifies a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet."[85] Direct allows secure email exchange of patient information between various organizations and individuals, such as providers and the government. However, patient and physician portals and robust identity management systems must be in place before patients can exchange their own data. The Direct Project is compatible with identity management that is voluntary and independent of any particular healthcare provider, but implementation problems could nullify Direct's full potential.

Currently, most HIEs rely on involuntary master patient indicies (MPIs) that make it easy for CEs and institutions to collect all patient data. Even if patients use the Direct Project and authorize data holders and data receivers to exchange PHI, the existence of MPIs makes patient control over PHI impossible. Ideally, patients alone will have all the "account numbers" for PHI held by data holders so they can control data sharing. Direct exchange should occur only between individuals, rather than between organizations.

More sophisticated consent systems can also use roles to help control disclosures. Roles linked to licensing authorities and clearly understood by the patient are an effective way to help achieve scalability and privacy.

Because Direct is based on a secure email system, patients can easily be contacted via cell phone or computer for secondary uses such as research.

Many states are adopting Direct to exchange data and meet the MU criteria for EHR certification, rather than using expensive, complex proprietary systems for data exchange. As of July 2012, more than 30 states are using Direct for HIEs.[86]

Wake Forest Health Researchers Build a Data Exchange Controlled by Patients

Recently, researchers at the Wake Forest School of Medicine's Department of Biomedical Engineering completed a small study[87] to demonstrate patient control over sharing image data between providers. They developed a health information exchange that works for providers and puts patients in control of transferring their medical images.

"An image sharing framework is described that involves patients as an integral part of, and with full control of, the image sharing process. Central to this framework is the Patient Controlled Access-key Registry (PCARE) which manages the access keys issued by image source facilities. When digitally signed by patients, the access keys are used by any requesting facility to retrieve the associated imaging data from the source facility. A centralized patient portal, called a PCARE patient control portal, allows patients to manage all the access keys in PCARE."[88]

Although the scale was small, the reasons for building systems so patients can transfer their own records are persuasive: speed; patients can be sure their records get to their own doctors; and there is no need for the complex, expensive contracts between entities that now control and exchange our data."[89]

'Blue Button': The Critical First Step to Restore Personal Control over Health Data

'Blue Button'[90, 91] is the name for the technical function that enables patients to see and download copies of their electronic health information. Patients' access to their own information was required by the HIPAA Privacy Rule in 2001. If patients cannot get personal health data (for example, via a Blue Button), they cannot use or control it, or check for errors.

Blue Button allows patients to collect and transfer their own data, ending 'data lock' by large health IT vendors, insurers, and hospital or provider systems.[92] Patients can also easily donate data for research they support.

The VHA Blue Button downloads have been used over one million times.[93] The ability to see and download electronic health information is very popular with the public. A further benefit of Blue Button is improved collaboration and communication between patients, families, and referring physicians, as well as saving staff time and costs of copying and mailing paper records.

In addition, the Automating Blue Button Initiative (ABBI) under the Standards and Interoperability (S&I) Framework is working to expand on the simple Blue Button concept. The S&I Framework is a collaborative community of participants from the public and private sectors who are focused on providing the tools, services, and guidance to facilitate the functional exchange of health information. ABBI is working to enhance the record format to provide for more machine-to-machine and automation potential. The initiative is also exploring "push" models that would automate the private and secure transmission of personal health data to a specific location of the consumer's choosing and "pull" models that would allow a third-party application of the consumer's choosing to privately and securely access personal health data on demand.[94]

RESTful Health Exchange (RHEx)[95] Could Be Used to Enable Patient Consent Management

"REST (REpresentational State Transfer)[96] is the dominant design paradigm used on the web that makes Google easy to search, Amazon easy to navigate, and E*TRADE secure.

"RHEx uses REST to make health information exchange simple and secure. By applying authentication standards widely used on the Internet, providers and patients can securely access trusted electronic health records with one account. RHEx supports a 'single sign-on' type environment."

Using RHEx, a patient can send a token to a health professional that allows that person to access to a particular document or a specified subset of their current EHR for a period of time. RHEx is also compatible with role-based access controls.

RHEx "uses web links to access existing patient data across trusted providers rather than duplicating information in a database. This construct enables a federated approach to data integration.[97]

"The RHEx design facilitates faster development at reduced costs. As an open-source solution, public and private developers can leverage RHEx and its benefits for a broad variety of healthcare solutions."

The use of patient-controlled models for data control and exchange fits the innovation paradigm proposed by Harvard business guru Clay Christensen (i.e., that innovation often starts with simple, less expensive market-based solutions).[98]

Currently, there are no simple off-the-shelf solutions to build privacy and patient control over PHI into the healthcare system. For example, even though the NDIIC open source consent modules offer good, existing technology for data segmentation, they would still have to be modified by engineers to fit with other EHRs. The government could fund modifications to enable major EHRs to use the NDIIC consent module and adapt this consent technology so that patients could set their own directives for disclosures, rather than using clinicians to type patient choices into EHR systems. Government should lead and fund building essential privacy infrastructure including patient and physician portals, choose a robust ID management system, fund research on factors that influence trust in electronic systems, and research electronic consent tools.

A 2011 paper by Mork, Rosenthal, and Stanford on "Architectures and Processes for Nationwide Patient-Centric Consent Management"[99] proposes an open-source consent service that includes detailed privacy preferences. The paper covers how requests could be managed, patient identifiers, inclusion of ancillary knowledge sources, a sample architecture for enforceable consent, and use cases that can work with fully automated systems or with manual systems receiving fax or mail requests for PHI. They concluded that "one could build a useful consent system today, whose main function was just to place consents (in machine and human readable form) on record holders' screens, and to automate the simplest cases (which are pleasantly common). Our architecture consciously avoided depending on universal participation, employment of data standards, record holder automation, or ancillary data completeness. Progress in these areas would permit greater automation, but in the near term, all tasks can be processed partly manually, with incremental automation. The system need not be perfect, just good enough to lure participants."[100]

Recently, the first government grant to fund consent technologies that enable segmentation for the exchange of sensitive data was announced in August 2012. Dr. Farzad Mostashari of ONC announced funding for a data-segmentation and consent pilot that will enforce the privacy rights of patients receiving drug or alcohol-abuse treatment through federally funded programs covered by 42 CFR Part 2.[101]

MYTHS ABOUT CONSENT

A number of prevalent myths are often used to justify the case for not building consent requirements into health IT systems and data exchanges.

Consent Weakens Privacy

Some argue reliance on patient consent weakens privacy because patients will agree to sign the same 'blanket' advance consents that have long been used in paper records systems. But this form of consent is illegal; it is impossible to give informed consent to disclose information that will be created in the future. Blanket consent was created for the paper age, when it was difficult, time consuming, and expensive to contact people individually for consent. Technology makes paper consents obsolete because contacting millions of people is easy, fast, and cheap.

Patients Are Incapable of Giving Informed Consent to Use PHI

Others argue that patients are incapable of making informed decisions about the use of their health records and are burdened by consent, especially during emergencies. This paternalistic approach shows a deep lack of respect for patients and supports institutional rather than patient control over PHI. Obtaining informed consent is actually the standard of practice in the United States. Physicians are trained to obtain consent under urgent circumstances and know it builds trust, so patients are willing to provide complete and accurate information.

Consent Is Too Costly and Complex

Industry complains that building in meaningful consent is too complex and costly. But what will it cost later?

"Environmental impact statements" are required when large-scale construction projects are proposed, so decision makers and the public can weigh the consequences before development starts. Why not require a similar process to evaluate the consequences of technology systems on patient control over PHI and privacy?

The costs of eliminating patient control over PHI in current electronic systems have not been calculated. What are the costs of treatment when millions avoid early diagnosis and treatment, cannot work, or suffer from disability or death? Who pays? What will it cost corporations, government, and elected officials when the public loses trust in the healthcare system?

The President's Council of Advisors on Science and Technology (PCAST) estimates the direct costs of building and maintaining a truly patient-centered, patient-controlled healthcare system would be $100-$300 million annually.[102] Compared to the billions in stimulus funds spent to build the nation's electronic healthcare system, these costs for a trustworthy system are reasonable.

Breakthrough Research, Population Health Research, and Bio-Surveillance Require Open Access to the Nation's PHI

Current health IT systems are designed to facilitate many kinds of research without patient knowledge or consent. Violating longstanding research ethics could very well backfire, producing widespread distrust of research and health IT.[103, 104]

As discussed earlier, Professor Alan Westin's survey for the IOM[105] found:

- Only 1 percent of the public would agree to research use of PHI without consent and an additional 8 percent would agree in advance to have their information used in future research.
- If the research study did not reveal their personal identities and was supervised by an IRB, only 19 percent of the public would agree to research use of PHI without consent.
- Importantly, 38 percent of respondents wanted each research project described to them and their specific consent obtained for each use.
- Minorities and other vulnerable populations were more negative about research use of data without consent than other groups.

The public deserves education about the real risks, as well as the benefits of disclosing sensitive health information for research. Researchers should "just ask" for consent.

AN IMPLEMENTATION PATH: FROM INSTITUTIONAL CONTROL TO INDIVIDUAL CONTROL IN FIVE YEARS

An optimal, patient-centered, trustworthy healthcare system could be built in five years. Technical tools, systems and legal changes, and public awareness are needed to achieve this goal.

There is no magic or simple solution. Various technologies and approaches could be used to implement trust and privacy in the healthcare system. Critically, new laws and enforcement of the ban on sales of PHI in HITECH are needed to stop corporations from surreptitiously collecting and selling intimate, detailed portraits of the mind and body of every adult in the United States.[106]

According to Stephan Brands, "While privacy can be enhanced by appropriate legislation and regulation, workable technical approaches, when they can be found, are often more effective."[107]

The optimal technology systems needed for trust and privacy are:

- **Patient and physician portals.** Portals are essential so patients can contact physicians and transfer selected health data to and from health professionals. The first step toward patient control over PHI is the ability to collect and transfer copies of all PHI.
- **Robust identity management controlled by patients.** Consumers should have a voluntary robust identity so physicians, health professionals, and researchers can reliably authenticate and contact them. A number of patient ID management systems would work well:
    - OAuth is an *open-source protocol* to allow *secure authorization* in a *simple* and *standard* method from web, mobile, and desktop applications.[108] OAuth is used by hundreds of millions of people even though they do not realize it.
    - OpenIDConnect[109] standards are also well worked out.
    - User Managed Access[110] (UMA) has a few pilots outside of healthcare and around the world.
    - Microsoft's open source UProve is "an innovative cryptographic technology that allows users to minimally disclose certified information about themselves when interacting with online resource providers. U-Prove provides a superset of the security features of Public Key Infrastructure (PKI), and also provides strong privacy protections by offering superior user control and preventing unwanted user tracking."[111]
    - When fully implemented, the National Strategy for Trusted Identities in Cyberspace Identity Ecosystem could be used for ID management. It offers a user-centric online environment, a set of technologies, policies, and agreed-upon standards that securely support transactions ranging from anonymous to fully authenticated and from low to high value.[112]
- **A single independent electronic consent management tool or system[113] for each patient** to ensure personal control over the use and disclosure of PHI (with rare statutory exceptions).
    - Patients should be able to set their robust consent preferences/directives in one place. All users and holders of PHI should be required to electronically verify each person's consent directives before using or disclosing any data.
    - Independent interactive consent management tools should allow consumers to exercise exquisite granular control of access to PHI (down to the data field in the future) and set individual and/or role-based access and time-limited access

for all users. Consumers must be able to see their actual data when setting consents so they can easily change their preferences.

- Robust education about setting up and using consent management tools should be embedded in the tools, so patients can learn about the risks and benefits of consent choices, understand and review any legal or ethical constraints on consent choices, and use default options to set or modify baseline directives (such as using consent directives recommended by trusted organizations or individuals). The default setting for all consent management systems should be the most privacy-protective set of preferences.
- Consent management tools permit consumers to instantly set or change their consents, set standing consent for data access in emergencies and routine situations (such as sending copies of all new health information to one's primary care physician but send only new medications and lab data to one's allergist, and/or allow access to all one's PHI by a specific researcher); set more narrow directives or preferences (such as do not allow a specific physician access to any of one's health data); and view complete audit trails of all uses and disclosures of their PHI. Patients can be contacted via cell phone or computer for any use or disclosure not covered by the patient's directives.
- Keeping all consents in a single independent location is convenient for consumers and makes it unnecessary to set up or remember to change consents with every health professional or entity that holds, stores, or transmits their personal health information. In addition, complete transparency and accountability for all data use is ensured because audit trails of disclosures of health records in one place makes patients' monitoring simple.

- **Health record banks.**[114] Health record banks are repositories for trustworthy copies of health information collected by the consumer. Patients own and control their health information in health record banks. They can collect, aggregate, and protect PHI and any information related to health (such as exercise, diet, environmental factors such as ozone levels, exposure to carcinogens in products, occupational hazards). Health record banks can transfer selected or complete health data wherever needed with patient consent. Health record banks and independent consent management tools will help fully protect every individual's right to health information privacy.

  Each person would have the ability to keep an up-to-date copy of their lifetime health records in a health record bank account. All access to the information in the account should be controlled only by the account-holder (the consumer), who would give permission for the necessary information to be available to healthcare providers. Each consumer can add and amend information as desired. All data would be marked as to the source of the information.

  Harvard's MyDataCan[115] "…puts your data under your control to improve your life. Patients can collect, assemble, and distribute their own personal data, across data silos, including health information, without a fee, and optionally elect to participate in activities that use your data to improve the quality of your life." According to the bank's director, Professor Latanya Sweeney, the database is doubly encrypted and

scalable to 300 million people. Those with accounts can use and learn from their own data via novel applications that analyze their data or be able to participate in research via applications.

- **Metadata-tagging could be used to enable patient control over PHI.**[116] The PCAST[117] identified "several barriers to innovation and vigorous competition in the market to create effective health IT systems." The PCAST recommendations for meta-data tagging offer a way that could ensure:
    - Patient privacy and control over PHI. The report acknowledged: "Legitimate patient concerns about privacy and security make patients uneasy about participating in health IT systems or granting consent for their information to be used in research."[118]
    - The ability to disaggregate, index, search, and assemble accurate information needed to treat patients.
    - Data are accessible in appropriate forms to patients, to patients' healthcare providers at other organizations, and in deidentified or aggregated form to public health agencies and researchers.
    - Health IT is oriented toward better care, not administrative functions.

An important benefit is that metadata can be aggregated and searched independently of the actual data.

Legal Changes Needed to Build an Optimal Patient-Centered, Trustworthy Healthcare System in Five Years

The President and Chief Technology Officer must direct relevant federal agencies to make the changes needed for trust in health IT and data exchange.

In order to strengthen patients' control over their PHI, privacy protections and foundational privacy-enhancing technologies and architectures could be added to the Meaningful Use regulatory requirements for EHRs or to new regulations promulgated and funded by HHS and the Centers for Medicare & Medicaid Services (CMS). The National Institutes of Health (NIH), CMS, and HHS could also fund pilots to test to effective electronic consent tools and patient-centered data exchange. In view of the urgency, the Presidential Executive Orders could be effective vehicles for some changes, and create pressure for new federal laws to

- **Restore a federal right of consent for all use and disclosures of PHI, establish tough penalties for noncompliance, and ensure that these requirements are vigorously enforced.**
- **Require health technology systems and applications to adhere to a robust trust framework such as the consumer-led Patient Privacy Rights (PPR) Trust Framework.**

  The PPR Framework built and tested by Microsoft and PriceWaterhouseCoopers includes 15 clear principles (and 75 auditable criteria that operationalize the principles):

  1. Easily find and understand privacy policy.
  2. Policy discloses how information is used and not used.

3. Requires explicit permission for data shared or sold.
4. Able to decide to participate or not.
5. Warned if data go to non-compliant third party.
6. Must agree to be contacted, profiled, tracked, or targeted.
7. Able to make field-level decisions about sharing.
8. Able to change any self-reported information.
9. Able to decide who has access to information.
10. Participation accessible to those with disabilities.
11. Easily find who accessed or used information.
12. Notified if information is lost, stolen, or breached.
13. Can easily report concerns and get questions answered.
14. Expect organization to punish misusers of information.
15. Expect data security.

- **Define the word 'privacy.'** Currently, Congress and the Administration have not chosen a definition of "privacy."[119, 120] Not having an official definition puts patients at a disadvantage. Without clarity regarding what is meant by privacy, it is open to misinterpretation and greatly complicates problem solving.
- **Strengthen enforcement of our existing strong state, federal, Constitutional, and ethical rights to control the use and disclosure of personal health information.** HITECH added tough, effective penalties for data breach but more is needed. Patients should also have a private right of action when entities violate their strong rights to control PHI or when entities fail to adequately protect data security and privacy.

  Clearly, federal agencies have not made enough use of the strong enforcement provisions in HIPAA and HITECH to protect the public. Fortunately, enforcement of the security requirements and the requirement for providing electronic copies of PHI has now begun. However, HHS has not yet released final regulations for other new consumer protections required by HITECH, including the accounting of disclosures of PHI from EHRs; the ban on the sale of PHI; and the requirement that if patients pay for treatment privately, they should be able to prevent disclosure of PHI to health plans.
- **Require a 'chain of custody' or map of data flows for PHI.** There can be no trust without verifying where personal data flows (accountability) and what it is used for (transparency). The HITECH requirement granting individuals' rights to obtain three years of Accounting of Disclosures of PHI from EHRs is clearly a start, but all disclosures of PHI from all data holders should also be auditable.

  Health information is used and disclosed by innumerable corporations and government agencies we do not know about; the need to build a health data map that identifies all hidden users of health data is urgent.[121] Individuals cannot weigh the benefits and risks of participating in health IT systems unless they know where their sensitive health information is located and what it is being used for. The federal government should fund research to develop a comprehensive map of health data flows.

- **Establish a 'second civil rights bill for the 21st century.'**[122] This civil rights bill should use the following principles, and Congress should require harms tests and enhanced "privacy impact statements" for all systems, data exchanges, applications, medical and mobile devices, and websites. The rights to privacy and to health information privacy are recognized as civil and human rights by the European Union (EU).[123] Detailed collection of data about individuals contributed to the horrors of World War II. The EU put tough data security and privacy protections in place to prevent future discrimination and atrocities.

  Technology systems and applications should not be built, sold, or used without first assessing the financial and human costs that result from specific IT systems, architectures, and applications.
- **Establish principles for protecting personal medical data.**[124] These principles should include
  - "Harmful acts must be clearly prohibited."
  - **"**The possession and use of personal medical data should be restricted without an individual's consent."
- **Adopt harms tests.**[125] This idea is similar to legal requirements for "environmental impact statements" to enable decision makers and the public to weigh the harms versus benefits of development and construction projects before approving them. It is good policy to map out unintended consequences before taking action. The use of enhanced "privacy impact statements" that specifically address harms would provide information needed to weigh decisions about technology and architecture.

CONCLUSION

Without meaningful, robust electronic consent management tools and robust privacy frameworks[126] in electronic systems, patients will not be able to control PHI, the most sensitive personal information of all. The lack of health information privacy should be the use case for building a truly privacy-preserving national technology infrastructure. We should never have to give up privacy to get health treatment. We must build privacy-enhancing technologies into all electronic health systems.

If you think about privacy carefully, the right to be "let alone"[127] is fundamental to democracy. The right to privacy must inevitably mean the right to control personally identifiable information about ourselves online and in electronic systems. We face a stark choice: will we preserve individual rights and the freedom to be let alone, or continue to accept hidden data flows?

References

1. Patient Privacy Rights' Data for Sale Slides. Available at: http://patientprivacyrights.org/wp-content/uploads/2012/10/PPR-Data-for-Sale-Deb-Peel-MD.pdf.
2. Avila J. Your Medical Records May Not Be Private. ABC News Investigation**.** September 13, 2012. Available at: http://abcnews.go.com/Health/medicalrecordsprivateabcnewsinvestigation/story?id=17228986#.UIQCz1H6Acs.

3. Duhigg C. How Companies Learn Your Secrets. *New York Times*. February 16, 2012. Available at: www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0.
4. Anderson C. *Free: The Future of a Radical Price.* 2009; page 104. (Practice Fusion's electronic health record application is featured as a case study for selling patient data, rather than licensing EHR technology.)
5. PriceWaterhouseCoopers. Old data learns new tricks: Managing patient security and privacy on a new data-sharing playground. September 2011. Available at: www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml; www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml.
6. Professor Latanya Sweeney explains theDataMap.org research project via video. Available at: www.healthprivacysummit.org/events/2012-health-privacy-summit/custom-138-ec40d08a35f947e487f68a5f534a9e82.aspx.
7. Mork P, et al. Architectures and Processes for Nationwide Patient-Centric Consent Management. Available at: www.docstoc.com/docs/125559003/Nationwide-Patient-Centric-Consent-Mgmt---v3--Approved-for-Public-Release.
8. Peel D. The case for informed consent: Why it is critical to honor what patients expect for health care, health it and privacy. August 2010. Available at: http://patientprivacyrights.org/wp-content/uploads/2010/08/The-Case-for-Informed-Consent.pdf.
9. 65 Fed. Reg. at 82,779, 65 Fed. Reg. at 82,777, 65 Fed. Reg. at 82,778.
10. National Consumer Health Privacy Survey. November, 2005. California Healthcare Foundation. Available at: www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.
11. Patient Privacy Right's Trust Framework; page 27.
12. Mork P, et al. Architectures and Processes for Nationwide Patient-Centric Consent Management. Available at: www.docstoc.com/docs/125559003/Nationwide-Patient-Centric-Consent-Mgmt---v3--Approved-for-Public-Release.
13. Patient Privacy Right's Trust Framework; page 27.
14. HIPAA regulations define health information as "any information, whether oral or recorded in any form or medium" that "(i)s created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and "(r)elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." Protected health information (PHI) under HIPAA includes any *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual (that's *identified* information). It also includes health information with data items which reasonably could be expected to allow individual identification. See: 45 CFR 160.103, 45 CFR 164.501.
15. NCVHS Report to HHS Secretary Michael Leavitt. Privacy and Confidentiality in the Nationwide Health Information Network. June 2006.
16. Westin A. *Privacy and Freedom*. 1966.
17. http://www.gpo.gov/fdsys/pkg/FR-1995-01-20/pdf/95-1480.pdf.
18. *Whalen v. Roe*, 97 S. Ct. 869, 877 (1977).
19. Terry N, et al. Ensuring the Privacy and Confidentiality of Electronic Health Records, 2007 U. Ill. L. Rev. 681-735. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=886904.
20. AHRQ Publication No. 09-0081-EF. Final Report: Consumer Engagement in Developing Electronic Health Information Systems. Prepared by Westat; July 2009. Available at: http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf.

21. HHS finding 65 Fed. Reg. at 82,464.
22. The State of Health Privacy, Health Privacy Project. 2000.
23. NCVHS Report to HHS. (June 22, 2006).
24. American Medical Association. Report 19 of the Board of Trustees (A-07), Patient Information in the Electronic Medical Record.
25. *Jaffee v. Redmond*, 116 S. Ct. 1923, 1929 (1996).
26. http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl.
27. *Olmstead v. United States*, 277 U.S. 438, 478, 48 S.Ct. 564, 572 (1928).
28. *Ferguson v. City of Charleston*, 532 U.S. 67, 121 S. Ct. 1281 (2001); *Whalen v. Roe*, 429 U.S. 589, 97 S. Ct. 869 (1977); *United States v. Scott*, 424 F.3d 888 (9th Cir. 2005); *Douglas v. Dobbs*, 419 F.3d 1097 (10th Cir. 2005); *Tucson Women's Clinic v. Eden*, 371 F.3d 1173 (9th Cir. 2004); *Gruenke v. Seip*, 225 F.3d 290 (3rd Cir. 2000).
29. Privacy Act of 1974, amendment added by section 2(a) (2) and (4) of Pub. L. 93-579: "Congress finds that…the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;… the right to privacy is a personal and fundamental right protected by the Constitution of the United States…". See also, 65 Fed. Reg. at 82,464 (December 28, 2000), "[p]rivacy is a fundamental right."
30. *Whalen v. Roe* 429 U.S. 589 (1977) at 596-605.
31. *Id*. *See also Id*. at 598-600, nn.22-26 (Noting that courts have recognized a privacy interest in avoiding disclosure of personal matters).
32. Supreme Court finding, *Jaffee v. Redmond* (95-266), 518 U.S. 1 (1996).
33. *Ibid*.
34. *Jaffee v. Redmond*, 116 S. Ct. 1923, 1929 (1996).
35. AHRQ Publication No. 09-0081-EF. Final Report: Consumer Engagement in Developing Electronic Health Information Systems. Prepared by Westat; July 2009. Available at: http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_888520_0_0_18/09-0081-EF.pdf.
36. Westin A. What Two Decades of Surveys Tell Us About Privacy and HIT. 1st International Summit on the Future of Health Privacy, June 13, 2010. Available at: https://custom.cvent.com/8C4BB5624279479B8D976E45540562FA/files/7d07e389dafd4bd8958a99668d93a19d.f.
37. Public comments by Blair Levin, former Broadband Chair for the FCC at the annual meeting of the Electronic Privacy Information Center's Privacy Coalition in 2010.
38. 65 Fed. Reg. 82,462.
39. 67 Fed. Reg. 53,183.
40. An example is "Julie" describing the reaction of a surgeon to reading notes about her child abuse in this video. Available at: www.healthprivacysummit.org/events/2012-health-privacy-summit/custom-137-ec40d08a35f947e487f68a5f534a9e82.aspx.
41. 67 Fed. Reg. at 53,212 (August 14, 2002).
42. www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.
43. *Ibid*.
44. California HealthCare Foundation, Consumer Health Privacy Survey; June 2005. Available at: www.chcf.org/topics/view.cfm?itemID=115694.
45. California HealthCare Foundation, National Consumer Survey on HIT; January, 2010. Available at: www.chcf.org/topics/view.cfm?itemID=134205.

46. 65 Fed. Reg. at 82,779.
47. 65 Fed. Reg. at 82,777.
48. 65 Fed. Reg. at 82,778.
49. *Invisible Wounds of War*. The RAND Corp. 2008; page 436.
50. *Ibid*.
51. Tarabay J. Suicide Rivals The Battlefield In Toll On U.S. Military. Available at: www.kpbs.org/news/2010/jun/17/suicide-rivals-battlefield-toll-us-military.
52. Cox E. Army pauses operations for mandatory suicide prevention training. See: http://articles.baltimoresun.com/2012-09-26/news/bs-md-army-suicides-2-20120926_1_suicide-rate-suicide-prevention-army.
53. Pewen W. Protecting our civil rights in the era of digital health. *The Atlantic*. August 2, 2012. Available at: www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343/#.
54. Patient Privacy Rights Data for Sale slides. Available at: http://patientprivacyrights.org/wp-content/uploads/2012/10/PPR-Data-for-Sale-Deb-Peel-MD.pdf.
55. HHS finding 65 Fed. Reg. at 82,472-473.
56. Professor Latanya Sweeney explains theDataMap.org research project via video. Available at: www.healthprivacysummit.org/events/2012-health-privacy-summit/custom-138-ec40d08a35f947e487f68a5f534a9e82.aspx.
57. Starr P. Health and the right to privacy. *American Journal of Law and Medicine*. 1999; 25:193-201.
58. National Consumer Health Privacy Survey, November, 2005, California Healthcare Foundation. Available at: www.chcf.org/publications/2005/11/national-consumer-health-privacy-survey-2005.
59. U.S. Public Opinion on Uses of Genetic Information and Genetic Discrimination, Genetics and Public Policy Center, April 24, 2007. Available at: www.dnapolicy.org/images/reportpdfs/GINAPublic_Opinion_Genetic_Information_Discrimination.pdf.
60. Westin A. What Two Decades of Surveys Tell Us About Privacy and HIT Today. Available at: http://tiny.cc/t2oblw.
61. Pewen W. Protecting Our Civil Rights in the Era of Digital Health. *The Atlantic*. August 2, 2012. Available at: www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343/#.
62. *Ibid*.
63. Westin AF. IOM Project Survey Findings on Health Research and Privacy. October 2, 2007. Available at: http://patientprivacyrights.org/media/WestinIOMSrvyRept.pdf?docID=2501.
64. HIPAA Standards for Privacy if Individually Identifiable Health Information, Final Rule 42 CFR Part 164.512(i) Use and Disclosure for Research, 64 Fed.Reg. at 82535.
65. National Consumer Health Privacy Survey. California Healthcare Foundation. November 2005. Available at: www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumerPrivacy2005Slides.pdf.
66. NCVHS Report to HHS. June 22, 2006.
67. Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of Helsinki, June 1964.
68. www.cdc.gov/mmwr/preview/mmwrhtml/su5201a1.htm .
69. Ethical Principles for Medical Research Involving Human Subjects, World Medical Association Declaration of Helsinki, June 1964.
70. See: www.systemedicus.com/ and http://rebarinteractive.com/electronic-informed-consent-types-technologies/.

71. PGP consent process. Available at: www.personalgenomes.org/consent/PGP_Consent_Approved03242009.pdf.
72. http://rebarinteractive.com/electronic-informed-consent-introduction/.
73. Mork P, et al. Architectures and Processes for Nationwide Patient-Centric Consent Management. Available at: www.docstoc.com/docs/125559003/Nationwide-Patient-Centric-Consent-Mgmt---v3--Approved-for-Public-Release.
74. *Ibid*.
75. Privacy and Security Tiger Team: Past Meetings, June 29, 2010, Consumer Choices Technology Hearing. Testimony and video available at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910.
76. PGP consent process. Available at: www.personalgenomes.org/consent/PGP_Consent_Approved03242009.pdf.
77. www.mdanderson.org/about-us/facts-and-history/institutional-profile/index.html.
78. https://my.mdanderson.org/selfenrollment.cfm.
79. http://us.linkedin.com/company/ndiic.
80. www.ndiic.com.
81. http://patientprivacyrights.org/wp-content/uploads/2012/10/Consumer-Choices-in-the-Clinical-Management-of-Behavioral-Health-Services-EHR.pdf. Accessed October 26, 2012.
82. For example, see: www.dshs.state.tx.us/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=8589946912 and www.dshs.state.tx.us/cmbhs/default.shtm. Accessed on October 26, 2012.
83. Privacy and Security TIGER Team: Past Meetings, June 29, 2010, Consumer Choices Technology Hearing. Testimony and video available at: http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=2833&PageID=19477#062910.
84. http://wiki.directproject.org/file/view/DirectProjectOverview.pdf.
85. *Ibid*.
86. www.fiercehealthit.com/story/onc-nearly-30-statewide-hies-using-direct-project/2012-06-19.
87. Ge Y, et al. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *J Am Med Inform Assoc*. August 11, 2012; doi:10.1136/amiajnl-2012-001146. Available at: jamia.bmj.com/content/early/2012/08/11/amiajnl-2012-001146.abstract.
88. *Ibid*.
89. Ge Y., et al. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *J Am Med Inform Assoc*. August 11, 2012; doi:10.1136/amiajnl-2012-001146.Available at: http://jamia.bmj.com/content/early/2012/08/11/amiajnl-2012-001146.abstract.
90. www.va.gov/bluebutton/.
91. www.healthit.gov/providers-professionals/faqs/what-blue-button-america.
92. http://wiki.siframework.org/ABBI+Push+Workgroup.
93. www.markle.org/publications/1679-video-blue-button-download-capability.
94. http://wiki.siframework.org/ABBI+Push+Workgroup. Accessed October 26, 2012.
95. http://wiki.siframework.org/RHEx.
96. *Ibid*.
97. *Ibid*.
98. Christensen C. *The Innovator's Dilemma, When New Technologies Cause Great Firms to Fail*. Harvard Business School Press; 1997.

99. Mork P, et al. Architectures and Processes for Nationwide Patient-Centric Consent Management. Available at: www.docstoc.com/docs/125559003/Nationwide-Patient-Centric-Consent-Mgmt---v3--Approved-for-Public-Release.

100. *Ibid*.

101. Conn J. HHS, VA go granular in info exchange demo. *Modern Healthcare*. September 17, 2012. Available at: www.modernhealthcare.com/article/20120917/NEWS/309179956.

102. PCAST Report. Available at: www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

103. Rothstein M. Improve Privacy in Research by Eliminating Informed Consent? IOM Report Misses the Mark. *Journal of Law, Medicine & Ethics*. 2010; 37(3):507-512.Available at: http://patientprivacyrights.org/wpcontent/uploads/2010/02/Rothstein-ReIOM-Report.pdf.

104. Harmon A. Indian tribe wins fight to limit research of its DNA. *The New York Times*. April 21, 2010. Available at: www.nytimes.com/2010/04/22/us/22dna.html?ref=us.

105. Westin AF. IOM Project Survey Findings on Health Research and Privacy. October 2, 2007. Available at: http://patientprivacyrights.org/media/WestinIOMSrvyRept.pdf?docID=2501.

106. Singer N. You for sale: mapping and sharing the consumer genome**.** *The New York Times*. June 16, 2012. Available at: www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=2&ref=business.

107. Brands S. *Rethinking Public Key Infrastructures and Digital Certificates, Building in Privacy.* 2000. Available at: www.credentica.com/the_mit_pressbook.html.

108. See: http://oauth.net.

109. http://openid.net.

110. http://kantarainitiative.org/confluence/display/uma/Home.

111. U-Prove, http://research.microsoft.com/en-us/projects/u-prove.

112. http://www.nist.gov/nstic/identity-ecosystem.html.

113. Mork P, et al. Architectures and Processes for Nationwide Patient-Centric Consent Management. Available at: www.docstoc.com/docs/125559003/Nationwide-Patient-Centric-Consent-Mgmt---v3--Approved-for-Public-Release.

114. www.healthbanking.org/pdf/principles.pdf.

115. http://mydatacan.org/.

116. For full PCAST report see: www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

117. www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf.

118. *Ibid*, page 2.

119. NCVHS Report to HHS Secretary Michael Leavitt Privacy and Confidentiality in the Nationwide Health Information Network. June 2006. Health information privacy is "an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data."

120. Westin A. Privacy and Freedom. 1966. "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."

121. Professor Latanya Sweeney explains theDataMap.org research project via video. Available at: www.healthprivacysummit.org/events/2012-health-privacy-summit/custom-138ec40d08a35f947e487f68a5f534a9e82.aspx.

122. Pewen W. Protecting Our Civil Rights in the Era of Digital Health. *The Atlantic.* August 2, 2012. Available at: www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343/#.

123. http://ec.europa.eu/dataprotectionofficer/legal_framework_en.htm.

124. Pewen W. Protecting Our Civil Rights in the Era of Digital Health. *The Atlantic.* August 2, 2012. Available at: www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343/#.

125. *Ibid*.

126. Patient Privacy Right's Trust Framework; page 27.

127. Brandeis dissent in *Olmstead v. United States*, 277 U.S. 438, 478, 48 S.Ct. 564, 572 (1928).

About the Book

Information Privacy in the Evolving Healthcare Environment is a critical book for health professionals or organizations interested in how the rapidly changing U.S. healthcare landscape will affect patient privacy. The book begins by discussing the meaning of privacy, the relationship between privacy and medical ethics; the synergy that exists between information privacy and security; and the complex legal landscape governing health information privacy. The book then shifts to explore some of the most significant privacy challenges faced by the healthcare community as it seeks to transform itself. Topics span from health information exchange and consent to secondary use and transparency. Finally, the book closes with a look to the future, identifying current trends and providing a view of the changes we might expect to see as a consequence of these trends.

With contributions by leading health privacy experts, *Information Privacy in the Evolving Healthcare Environment* was written in a style that is easy to grasp for professionals across the healthcare spectrum, including physicians, health IT professionals, administrators, and policymakers.

About the Editor

Linda Koontz, CIPP/US, CIPP/G, is a Senior Principal for Privacy and Strategy at MITRE, a not-for-profit corporation chartered to work solely in the public interest, which operates multiple Federally Funded Research and Development Centers (FFRDC). In this role, she leads the strategic privacy work for MITRE's Center for Connected Government, advising senior-level staff at federal agencies on strategic approaches to building privacy into their organizations, processes, and systems. She currently advises the Chief Privacy Officer of the Office of the National Coordinator on privacy issues associated with nationwide implementation of health information exchange and manages the activities of the Health Information Technology Policy Committee's Privacy and Security TIGER Team. She has also provided privacy advice and support to the Department of Homeland Security and was recently appointed by the Secretary to the Department's Data Protection and Integrity Advisory Committee (DPIAC).

Ms. Koontz has more than 30 years' experience in information systems management and technology. Prior to joining MITRE, she served as the Director, Information Management, for the U.S. Government Accountability Office (GAO). In that role, she directed a broad portfolio of congressionally-requested studies, producing numerous reports on privacy, information access and dissemination, information collection, and records management. Ms. Koontz also testified numerous times before congressional committees as an expert witness on these issues. She holds a BA in Accounting from Michigan State University and is a Certified Information Privacy Professional. She is also an Executive Coach and a graduate of Georgetown University's Leadership Coaching Program.

About HIMSS

HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of health and healthcare. Founded 52 years ago, HIMSS and its related organizations are headquartered in Chicago with additional offices in the United States, Europe and Asia. HIMSS represents more than 52,000 individual members, of which more than two thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 600 corporate members and more than 225 not-for-profit partner organizations that share our mission of transforming healthcare through the best use of information technology and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, research initiatives, and media vehicles designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care. To learn more about HIMSS and to find out how to join us and our members in advancing our cause, please visit our website at www.himss.org.

HIMSS®

33 W. Monroe St., Suite 1700
Chicago, IL 60603-5616
312-915-9282
www.himss.org

Order Code: 626

ISBN 978-1-938904-36-3
$90.00
59000
9 781938 904363